International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 01 | Jan -2017 www.irjet.net p-ISSN: 2395-0072

EPLQ:EFFICIENT PRIVACY PRESERVING SPATIAL RANGE QUERY FOR SMART PHONES

Pavitra Parjane[1], Pratiksha Raut[2], Priti Singh[3] , Harshada Wadile[4]

[1,2,3 & 4] *BE(Student), Information Technology, NDMVP's KBTCOE, Unipune university, Maharashtra, India*

Abstract - *The smart phones more popular and important in the users day-to-day life with the increasing development in technology in smart phones, the use of location based services have been increased in the recent years and also grabbing the attentions of the people . In our work, using the spatial range query and also the location based query which will provide the information and contents to the user according to his/her point of interest[1]. Our work aims to give the location to the user according to his point of interest with a dynamic range. Also the user's location is also provided security. For reducing the latency in the in the work we are going to design a privacy-preserving tree index structure in efficient privacy preserving location. The detail security analysis will confirm the security properties of efficient privacy preserving location. By performing various experiment we conclude that EPLQ is very efficient in privacy preserving spatial range query over out sourced data.*

Key Words*: *Location-based services (LBS), Outsourced encrypted data, Privacy-enhancing technology , Spatial range query

1.INTRODUCTION

The time of advance technologies and services, location access is one of the important feature. The accessing of the location via using several technologies has made it life easy at the industrial as well as the domestic level. The Location-based services is one of the software level service which is used to determine the Point of interest (POIs) within the given range of the individual's distance [2]. The LBS helps in determining the location of any person[4], object or any activity which is being held at a particular location. The Industrial sectors has greatly benefited from the use of LBS software especially in the operational and banking sectors usually helping out to determine the locations of ATMs, online wire transfer, etc. Due to its tremendous benefits to the industrial[6], social and individual level it has become ever growing trend in the recent times to outsource the use of LBS. There always comes a bane with the boon using the advanced technologies. In most of the LBS software it is necessary for users to submit their locations, which increases the concerns on issues about leaking and misusing the user location data. This loophole of the LBS has led to several social calamities in criminal activities, Trade secrets and as high as to national security. With the ever growing use of the LBS it has become absolutely essential to protect the privacy of user location. With the outsourcing of the LBS in the recent times it has raised several challenges which are as follows:

1.Challenge on querying encrypted LBS data.
2.Challenge on the resource consumption.
3.Challenge on the efficiency of POI searching.
4.Challenge on security.

2. LITERATURE SURVEY

1) Anonymity can provide a high degree of privacy, save service users from dealing with service providers privacy policies, and reduce the service providers requirements for safe guarding private information. We construct public-key systems that support comparison queries. On encrypted data as well as more general queries such as subset queries. These systems support arbitrary conjunctive queries without leaking information on individual conjuncts. In addition, we present a general framework for constructing and analysing public-key systems supporting queries on encrypted data[2].

2) In Secure KNN computation on encrypted database[4] , service providers like Google and Amazon are moving into the Software as a Service business. They turn their huge infrastructure into a cloud-computing environment and aggressively recruited businesses to run applications on their respective platforms. To enforce security and privacy on such the service model, we need to provide protection to the data running on the platforms. Unfortunately,

traditional encryption methods that aim at providing unbreakable protection are often not adequate because they do not support the execution of applications such as database queries on the encrypted data. In Secure KNN computation on encrypted database the general problem of secure computation on an encrypted database and propose a SCONEDB (Secure Computation ON an Encrypted DataBase)

Table-1: Literature Survey

Literature Survey			
Sr no.	**Details of the paper**	**Work Reported**	**Research Gap Identified**
1.	EPLQ: Efficient Privacy-Preserving Location-based Query over Outsourced Encrypted Data.	EPLQ: Efficient Privacy Preserving Location-based Query over Outsourced Encrypted Data.	In this paper , they have introduced the static range for searching the records as per user's point of interest . We will provide the dynamic range for searching the records and also secure the users location with the help of encryption techniques.
2.	Similarity indexing with the ss-tree.	Reported on ss-tree algorithm	With the help of ss-tree algorithm, it gives limited no. of records. We will provide the dynamic range for searching so that the number of records will increase automatically

model, which captures the execution and security requirements. The focus was on the problem of k-nearest neighbor (KNN) computation on an encrypted database. They developed a new asymmetric scalar-product-preserving encryption (ASPE) that preserves a special type of scalar product. They used APSE to construct two secure schemes that support KNN computation on encrypted data; each of the schemes shows resistance of practical attacks of a different background knowledge level, at a different overhead cost.

3) A. Gutscher proposes Private[7], a distributed architecture for anonymous location-based queries, which addresses the problems of existing systems. (i) Develop a superior K-ASR construction mechanism that guarantees query anonymity even if the attacker knows the location of all user. (ii) Introduce a distributed protocol used by mobile entity to self-organize into a fault-tolerant overlay network. In Private, K-ASRs are built in a decentralized fashion, therefore the bottleneck of the centralized server is avoided. Since the state of the system is distributed, Private is resilient to attacks. This approach hurts the accuracy and timeliness of the responses from the Server. B.Hoh the challenge of providing strong privacy guarantees while maintaining high data accuracy of time-series location data. Specifically, the key contributions of this work are: 1. Introduction of a novel time-to-confusion metric to evaluate privacy in a set of location traces. 2. Development of an uncertainty-aware privacy algorithm that can guarantee a specified maximum time-to-confusion.

4) Order Preserving Encryption for Numeric Data Rakesh Agrawal,Jerry Kiernan,Ramakrishnan Srikant,Yirong Xu [8], Encryption is a well established technology for protecting sensitive data. However, once encrypted, data can no longer be easily queried aside from exact matches. We present an order-preserving encryption scheme for numeric data that allows any comparison operation to be directly applied on encrypted data. Query results produced are sound (no false hits) and complete (no false drops). Our scheme handles updates gracefully and new values can be added without requiring changes in the encryption of other values. It allows standard database indexes to be built over encrypted tables and can easily be integrated with existing database systems. The proposed scheme has been designed to be deployed in application environments in which the intruder can get access to the encrypted database, but does not have prior domain information such as the distribution of values and cannot encrypt or decrypt arbitrary values of his choice. The encryption is robust against estimation of the true value in such environments.

3. CONCLUSIONS

An efficient privacy preserving spatial range query solution for smart phones ,which preserves the privacy of user location,and achieves confidentiality of Location based solution data. To realize EPLQ, we have designed a novel predicate-only encryption scheme for inner product range named IPRE and a novel privacy-preserving index tree named ss-tree. EPLQs efficiency has been evaluated with theoretical analysis and experiments, and detailed analysis shows its security against known-sample attacks and cipher text-only attacks. the techniques that the advantage uses in all other kind of preserving queries also which can helpful in the development of project . In future , the server will provide the result and information as per the user point of interest. The user can search any information related to school, hospital, ATM ,hotels. Futher we will extent our database. We are going to make our range dynamic for search and also we will collect the more data as much as possible.

REFERENCES

[1] EPLQ: Efficient Privacy-Preserving Location-Based Query Over Outsourced Encrypted Data Lichun Li, Rongxing Lu, Senior Member, IEEE, and Cheng Huang,APRIL 2016.

[2] D. Boneh and B. Waters, Conjunctive, subset, and range queries on encrypted data,in Theory of Cryptography, 4th Theory of Cryptography Conference, TCC 2007,Amsterdam,The Netherlands, February 21-24, 2007, Proceedings, 2007, pp. 535554.

[3] A. Boldyreva, N. Chenette, Y. Lee, and A. Oneill, Order-preserving symmetric encryption, in EUROCRYPT. Springer, 2009, pp. 224241.

[4] W. K. Wong, D. W.-l. Cheung, B. Kao, and N. Mamoulis, Secure kNN computation on encrypted databases, in Proc. SIGMOD, 2009, pp. 139152.

[5] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, Private queries in location based services: Anonymizers are not necessary, in Proc. SIGMOD, 2008,pp. 121132.

[6] J. Shao, R. Lu, and X. Lin, Fine: A _ne-grained privacy-preserving location-based service framework for mobile devices, in INFOCOM. IEEE, 2014.

[7] A. Gutscher, Coordinate transformation - a solution for the privacy problem of location based services? in 20th International Parallel and Distributed Processing Symposium (IPDPS 2006), Proceedings,25-29 April 2006, Rhodes Island, Greece, 2006.

[8] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, Order preserving encryption for numeric data, in SIGMOD. ACM, 2004.